

REGENSTRIEF INSTITUTE, INC

Public Health Emergency Surveillance System

Support Plan

PUBLIC HEALTH EMERGENCY SURVEILLANCE SYSTEM (PHESS)

Support Plan

© Regenstrief Institute, Inc.
1050 Wishard Blvd. • Indianapolis • Indiana 46202
Phone 317.630.7400 • Fax 317.630.6962

Table of Contents

Attachment A Section 3.1 Item B	1
(A) How the support plan will involve hospital and state personnel	1
(B) Notification, response and escalation procedures in the event of an outage	1
(B)1. Regenstrief to ISDH	2
(B)2. Hospital to Regenstrief	2
(C) Disaster Recovery Procedures	3
(D) Service Warranties	3
(E) Service Level Agreement	3

Attachment A Section 3.1 Item B

Contractor shall prepare a support plan of how the Collection System will be supported by Contractor, including at a minimum: (a) how it will involve hospital and ISDH personnel; (b) notification, response and escalation procedures in the event of an outage; (c) disaster recovery procedures, (d) outline of any hardware, software, and service warranties Contractor is willing to make, and (e) Contractor's service level agreement. If Contractor recommends a change to the support strategy or specifics change, then Contractor shall update the support plan document and deliver it to ISDH for approval.

A. How the support plan will involve hospital and state personnel.

In the event that data transfer between Regenstrief and the ISDH is unsuccessful, Regenstrief will contact the designated individuals at the ISDH after first verifying that Regenstrief's system is operational. In the event that data transfer between a connected hospital and Regenstrief is unsuccessful, Regenstrief will contact designated individuals at the hospital after first verifying that the Regenstrief's system is operational. If Regenstrief is unable to notify designated hospital personnel, they will solicit the assistance of the ISDH to notify the appropriate personnel.

B. Notification, response and escalation procedures in the event of an outage

There are two general types of outages to consider. The first is an outage between Regenstrief and the ISDH, the second is an outage between Regenstrief and a hospital.

(B)1. Regenstrief to ISDH

Regenstrief has developed an automated data transfer process that alerts our System Engineer and other stakeholders (including ISDH PHESS personnel) when scheduled data transfer is unsuccessful. In the event that data transmission between Regenstrief and the ISDH is interrupted, Regenstrief will first verify that their connectivity hardware and software is operational. Next, Regenstrief will verify that connectivity to the ISDH is functional. If internal troubleshooting and connectivity testing fails to identify the problem, Regenstrief will escalate by contacting designated individuals at the ISDH and work with them to resolve the issue.

(B)2. Hospital to Regenstrief

When a hospital's data transmission ceases or drops below expected thresholds, Regenstrief will initially verify that the hospitals' message listener for the given hospital is operational. In the event that the message listener is down, Regenstrief will attempt to restart the message listener.

If restarting a down message listener does not resolve the issue, Regenstrief will next verify that network connectivity is still established with the hospital. In the event that connectivity between Regenstrief and the hospital is down, Regenstrief will contact hospital networking personnel to re-establish secure connectivity.

If all processes on Regenstrief's end are operational, we will work with the hospital to ensure that connectivity is established at their end and verify that their message sender (which is typically a commercial interface engine) is operational and transmitting data.

If Regenstrief is unsuccessful notifying designated hospital personnel, they will solicit the assistance of the ISDH to make contact with the hospital. When message flow interruption is detected and is expected

to take more than one hour to remedy, the state will be notified. Intermittent outages that are immediately resolved will be noted in monthly progress reports.

C. Disaster Recovery Procedures

In case of a catastrophic hardware failure of Regenstrief's core message processor server, one of four failover servers will assume message processing tasks until the primary server is restored. PHESS data, programs and disk images are backed up on a routine basis and stored at a remote site. The backups can be used to restore or build a new system to handle surveillance data.

There are two MS Windows servers (primary and failover) responsible for transferring accumulated data to ISDH. In the unusual event that both servers fail, the data transfer process can be installed on any of multiple other MS Windows servers.

D. Service Warranties

Service warranty is covered by service level agreement in item E.

E. Service Level Agreement

The Regenstrief Institute (RI) will transmit to ISDH any new data available from hospitals once every three hours or at another mutually agreeable interval. There may be some interruptions in the schedule for scheduled downtime for any problems outside of RI's control. Further, RI is not responsible for the failure of one or more hospitals or other data providers to send the data to RI. RI is also not responsible for problems with the communication line between ISDH and RI.